REMARKS

Please reconsider this application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of the Claims

Claims 1-8 are pending in this application. Claims 1, 5, and 8 are independent. The remaining claims depend, directly or indirectly, from the independent claims.

Amendments to the Specification

The specification has been amended to correct a typographical error in accordance with the Examiner's suggestion. Specifically, paragraph [0031] of the specification has been amended to replace reference "**43**" with "**34**" to conform to Figure 4. No new matter has been added by this amendment.

Amendments to the Claims

Claims 1, 5, and 8 have been amended by way of this reply to clarify the claimed invention. No new matter has been added by these amendments. Support may be found in the original claims and the published specification.

Rejection(s) under 35 U.S.C. § 103

Claims 1-8 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,481,610 ("Doiron") in view of U.S. Patent No. 6,883,097 ("Lotspiech"). To the extent this rejection may still apply to the amended claims, this rejection is respectfully traversed.

The present invention relates to "equipment for DVD capable of protecting prescribed information such as a password or key data for encryption or decryption recorded in a memory, and a method and an apparatus for recording the prescribed information." *See* paragraph [0002] of the published specification. "An object of the present invention is to provide equipment for DVD capable of protecting prescribed information such as key data stored in a memory against copy or peeping." *See* paragraph [0008] of the published specification. As such, "the present invention includes a memory in which key data associated with information on a DVD is recorded in advance, and a processing portion processing information on the DVD using the key data from the memory. In the memory, random data is written around the key data." *See* paragraph [0009] of the published specification.

The key data may serve as an encryption key for equipment that encrypts and records information on a DVD. *See* paragraph [0011] of the published specification. The key data may also serve as a decryption key for equipment that decrypts information read from a DVD. *See* paragraph [0012] of the published specification. In addition, "the key data is recorded buried in the random data in the memory, a third party cannot identify and read the key data from the memory. Therefore, the key data stored in the memory can be protected against copy or peeping." *See* paragraph [0010] of the published specification. Moreover, the key data can be modified by a key data writing equipment.

Accordingly, claim 1, as amended, recites, in part, "the key data can be modified by a key data writing equipment." Amended claims 5 and 8 recite, in part, substantially similar limitations to that of claim 1 noted above.

In the Description of the Background Art of the present specification, Japanese Patent Laying-Open No. 2002-16593 discloses technology for encryption and decryption using a key and encryption processing based on key information. Japanese Patent Laying-Open No. 2002-73420 discloses an encryption key used to encrypt data of which copyright should be protected. Further, the use of Media Key Blocks ("MKBs") is disclosed. MKBs enable a disc to implicitly authenticate the device that is trying to play it. In the MKB scheme, licensed media manufacturers are provided keys to store on the disc to be protected. Additionally, compliant devices are given a unique set of keys. If a device has a valid set of keys, it is able to process the MKB and derive the cryptographic key that is used to decrypt the content stored on the disc. If the device is not a compliant device, it will not be able to read the protected disc. If a key is stolen from a complaint player through reverse engineering or other approach, the licensor issues new MKBs to all licensed media manufacturers that disables the stolen device key. As such, if a device with a stolen key attempts to read one of the newer discs with an updated MKB, the MKB data structure triggers the device to calculate an incorrect key, thus preventing the player from decrypting the content. Thus, the MKB scheme contemplates that keys may be improperly obtained and addresses this issue through a process that disables the device from playing back subsequently modified discs.

Doiron relates to digital radios having a secure mode that encrypts and decrypts messages. Specifically, Doiron discloses the use of cryptographic keys stored in non-volatile memory to encrypt and decrypt messages related to digital radios. The Examiner admits that Doiron does not disclose the information stored on a digital video disc or the writing of random data around the key in memory. As such, the Examiner cites Lotspiech as providing that which Doiron

lacks. Specifically, the Examiner states that Lotspiech discloses the use of media key blocks for encrypting information on recordable media and hiding of cryptographic keys in pseudo-random data.

The Applicant respectfully asserts that the Examiner has mischaracterized the claimed invention. The Description of the Background Art of the present specification discusses the use of cryptographic keys to encrypt and decrypt data and the MKB scheme of copy protection. In the MKB scheme, once a device key is improperly obtained from a device, the recourse is for the licensor to modify the MKB key in all subsequently manufactured discs in a way that disallows playback of the subsequent discs with the modified MKB key on a device using the improperly obtained device key. As such, Doiron and Lotspiech merely disclose, at most, that which is described in the Description of the Background Art of the present specification.

In contrast, the claimed invention relates to a device comprised of memory in which key data associated with information on a digital video disc is recorded in advance, means for processing the information on the digital video disc using the key read from the memory, wherein the random data is written around the key data in memory, and *the key data can be modified by a key data writing equipment.* In addition, the claimed invention teaches a method and apparatus by which the key data can be written to memory. As such, the independent claims, as amended, provide a mechanism for hiding a key in memory and a mechanism by which that key can be modified should the device key be improperly obtained and render the device inoperable with subsequently modified discs. Doiron fails to disclose the above stated limitations of the claimed

invention. Moreover, Lotspiech fails to provide that which Doiron lacks, as is evidenced by the fact that the Examiner relies upon Lotspiech merely to disclose the use of media key blocks.

In view of the above, independent claims 1, 5, and 8 are patentable over Doiron and Lotspiech, whether considered separately or in combination for at least the reasons set forth above. Dependent claims 2-4 and 6-7 are allowable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 04536/034001).

Dated: February 25, 2008

Respectfully submitted,

By _____

Jonathan P. Osha
Registration No.: 33,986
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant